Application No.: 10/721,079 Docket No.: 4590-239

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended): A random number generator adapted to receive an input of a number of bits coming from a physical source, wherein the generator comprising, in combination:

at least one symbol-generating physical source;

an arithmetic encoder; and

smoothing means adapted to smooth the residual output biases[[.]];

wherein the arithmetic encoder comprises at least one table of statistics on the input symbols receiving a piece of information on contexts, several registers, one comparator and one logic unit.

- 2. (Previously presented): The generator according to claim 1, wherein the smoothing means is constituted by a linear output function enabling the smoothing of the residual output biases.
 - 3. (Cancelled)
- 4. (Original): The generator according to claim 1, wherein the smoothing means comprises a register, a serial input and a parallel output.
- 5. (Currently amended): A method for the generation of random numbers comprising the following steps:

reception of several symbols from a physical source;

transmission of the symbols to an arithmetic encoder step; and smoothing the encoded symbols using a linear function[[.]]:

encoding the symbols by a number derived from computations of nested intervals, an interval [ms, Ms] corresponding to a symbol s and having a size proportional to its frequency of occurrence.

Application No.: 10/721,079

Docket No.: 4590-239

- 6. (Cancelled)
- 7. (Previously presented): The method according to claim 5, further comprising: updating a table of statistics on the input symbols as a function of the contexts; computing the new values of the boundaries of the interval [ms, Ms] by a rule of three; and

emptying the registers of the most significant bits that they have in common.

- 8. (Previously presented): The method according to claim 5, wherein the encoding comprises the following steps:
 - 1. initializing $m \to 0$ and $M \to 1$
 - 2. updating, for each symbol s of the message to be compressed:

$$\Delta \leftarrow M - m ;$$

$$m \leftarrow m + \Delta \times m_s ;$$

$$M \leftarrow m + \Delta \times M.$$

- 3. choosing the compressed message as being the last value of m.
- 9. (Currently amended): The generator method according to claim 5 wherein the smoothing function makes use of a polynomial which is, at most, a 15th degree polynomial.
 - 10. (Cancelled)
- 11. (Currently amended): The method generator according to claim 2, wherein the smoothing means comprises a register, a serial input and a parallel output.
- 12. (Original): The method according to claim 7, wherein the contexts are previous symbols.